IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of

PAUL C. KOCHER et al.

Application No.: 10/005,105

Filed: December 3, 2001

For: DIFFERENTIAL POWER ANALYSIS METHOD AND APPARATUS

Confirmation No.: 1675

Group Art Unit: 2132

Examiner: Justin T. Darrow

Attorney Docket No 44424162-8721

SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT

SONNENSCHEIN NATH & ROSENTHAL LLP
Customer No. 26263

M/S RCE
Commissioner for Patents
P.O. Box 1450
Arlington, VA 22313-1450

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail in an envelope, addressed to: M/S RCE, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on Dec 20 2005.

SONNENSCHEIN NATH & ROSENTHAL LLP

Dated: Dec 20 /05 By: Edward Radlo
Edward J. Radlo

Sir:

Applicant(s) submit(s) herewith patents, publications or other information [attached hereto and listed on the attached Form PTO-1449 (modified)] of which they are aware, which they believe(s) may be material to the examination of this application and in respect of which there may be a duty to disclose in accordance with 37 CFR § 1.56.

This Information Disclosure Statement:

(a) ☐ accompanies the new patent application submitted herewith. 37 CFR § 1.97(a).

(b) ☐ is filed within three months after the filing date of the application or within three months after the date of entry of the national stage of a PCT application as set forth in 37 CFR § 1.491.

(c) ☒ as far as is known to the undersigned, is filed before the mailing date of a first Office Action on the merits, or before a first office action after filing a Request for Continued Examination under §1.114.

complies with 37 CFR § 1.98 and MPEP § 609 and the Examiner is respectfully requested to consider the listed references.

The Commissioner is hereby authorized to charge our Deposit Account No. 19-3140, for any fees required in connection with the filing of this Information Disclosure Statement. **A duplicate copy of this Notice is enclosed for this purpose**. In particular, in the event that an Office Action has crossed in the mail with this Information Disclosure Statement, the Commissioner is authorized to charge the above-named deposit account for any fees required pursuant to CFR §§ 1.17(p) or 1.17(i)(1).

Respectfully submitted,

date of signature: Dec. 20, 2005

Edward J. Radlo, Reg. No. 26,793
Attorney of Record

SONNENSCHEIN NATH & ROSENTHAL LLP
P.O. Box 061080
Wacker Drive Station, Sears Tower
Chicago, Illinois 60606-1080
(415) 882-2402

enclosures

cc: J. Yang (w/encl.)
P. Kocher (w/encl.)
IP/T docket CH (w/o encl.)

(d) ☐ is filed after the first office action and more than three months after the application's filing date or PCT national stage date of entry filing but, as far as is known to the undersigned, prior to the mailing date of either a final rejection or a notice of allowance, whichever occurs first, and is accompanied by either the fee ($180) set forth in 37 CFR § 1.17(p) or a certification as specified in 37 CFR § 1.97(e), as checked below.

(e) ☐ is filed after the mailing date of either a final rejection or a notice of allowance, whichever occurred first, and the Issue Fee has not been paid, and is accompanied by the fee ($130) set forth in 37 CFR § 1.17(p)(1) and a certification as specified in 37 CFR § 1.97(e), as checked below. This document is to be considered as a petition requesting consideration of the information disclosure statement.

A list of the patent(s) or publication(s) is set forth on the attached Form PTO-1449 (Modified). A copy of the items on PTO-1449 (Modified) is supplied herewith, except for issued United States Patents and Published United States Patent Applications.

A concise explanation of relevance of the items listed on form PTO-1449 (Modified) is:

(h) ☒ not given

(i) ☐ given for each listed item

(j) ☐ given for only non-English language listed item(s) [Required]

(k) ☐ is in the form of an English language copy of a Search Report from a foreign patent office, issued in a counterpart application, which refers to the relevant portions of the references [copy attached].

The Examiner is reminded that a "concise explanation of the relevance" of the submitted items "may be nothing more than identification of the particular figure or paragraph of the patent or publication which has some relation to the claimed invention," MPEP § 609.

While the information and references disclosed in this Information Disclosure Statement may be "material" pursuant to 37 CFR § 1.56, it is not intended to constitute an admission that any patent, publication or other information referred to therein is "prior art" for this invention unless specifically designated as such.

In accordance with 37 CFR § 1.97(g), the filing of this Information Disclosure Statement shall not be construed to mean that a search has been made or that no other material information as defined in 37 CFR § 1.56(a) exists. It is submitted that the Information Disclosure Statement

PTO/SB/08a (08-03)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of info unless it contains a valid OMB control number.

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet 1 of 2

Complete if Known	
Application Number	10/005,105
Filing Date	December 3, 2001
First Named Inventor	Paul C. Kocher
Group Art Unit	2132
Examiner Name	Justin T. Darrow
Attorney Docket No.r	44424162-8721

OTHER ITEMS – NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		Posting on sci.crypt newsgroup, RIVEST, Ron, "Announce: Timing cryptanalysis of RSA, DH, DSS", 12-11-95, retrieved from internet 11-19-05, http://groups.google,com/group/sci.crypt/msg/79e75dc930adf?dmode=source&hl=en.	
		Posting on sci.crypt newsgroup, KOCHER, Paul C, "Announce: Timing cryptanalysis of RSA, DH, DSS", 12-11-95, retrieved from internet 11-19-05, http://groups.google,com/group/sci.crypt/msg/027dadba758893a5?dmode=source&hl=en.	
		Posting on sci.crypt newsgroup, WALTERS, Jim, "Announce: Timing cryptanalysis of RSA, DH, DSS", 12-11-95, retrieved from internet 11-19-05, http://groups.google,com/group/sci.crypt/msg/77b761989c18baea?dmode=source&hl=en.	
		Posting on sci.crypt newsgroup, KOCHER, Paul C, "Announce: Timing cryptanalysis of RSA, DH, DSS", 12-12-95, retrieved from internet 11-22-05, http://groups.google,com/group/sci.crypt/msg/769112d9a7a17488?dmode=source&hl=en.	
		Posting on sci.crypt newsgroup, RUBIN, Paul, "Announce: Timing cryptanalysis of RSA, DH, DSS", 12-12-95, retrieved from internet 11-22-05, http://groups.google,com/group/sci.crypt/msg/7c8fva520b1b5482?dmode=source&hl=en.	
		Posting on sci.crypt newsgroup, BROWN, Ralf, "Announce: Timing cryptanalysis of RSA, DH, DSS", 12-12-95, retrieved from internet 11-22-05, http://groups.google,com/group/sci.crypt/msg/417b42c49fe7cf53?dmode=source&hl=en.	
		Posting on sci.crypt newsgroup, STEWART, Bill, "Announce: Timing cryptanalysis of RSA, DH, DSS", 12-13-95, retrieved from internet 11-22-05, http://groups.google,com/group/sci.crypt/msg/7610aea60249ed48?dmode=source&hl=en.	
		Posting on sci.crypt newsgroup, Larry, "Announce: Timing cryptanalysis of RSA, DH, DSS", 12-15-95, retrieved from internet 11-22-05, http://groups.google,com/group/sci.crypt/msg/ced8289a35a32925?dmode=source&hl=en.	
		Posting on sci.crypt newsgroup, COSTA, Bob, "Re: Attacking machines on the Internet (re: Timing cryptanalysis of RSA, DH, DSS)", 12-16-95, retrieved from internet 11-22-05, http://groups.google,com/group/sci.crypt/msg/350820497cce62ba?dmode=source&hl=en.	

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unqiue citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/SB/08a (08-03)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Substitute for form 1449B/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet 2 of 2

Complete if Known	
Application Number	10/005,105
Filing Date	December 3, 2001
First Named Inventor	Paul C. Kocher
Group Art Unit	2132
Examiner Name	Justin T. Darrow
Attorney Docket No.	44424162-8721

OTHER ITEMS – NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		Posting on sci.crypt newsgroup, PERRY, Tom, "Announce: Timing cryptanalysis of RSA, DH, DSS", 12-17-95, retrieved from internet 11-22-05, http://groups.google,com/group/sci.crypt/msg/20e43912653f9bd0?dmode=source&hl=en.	
		Posting on sci.crypt newsgroup, BELL, Jim, "Spread-Spectrum computer clock?", 12-24-95, retrieved from internet 11-22-05, http://groups.google,com/group/sci.crypt/msg/485abca33cc29703?dmode=source&hl=en.	
		Posting on mail.cypherpunks, BRANDT, Eli, "Re: Timing Attacks", 12-11-95, retrieved from internet 12-7-05, http://groups.google.com/group/mail.cypherpunks/msg/fa276adeb23f2b83?dmode=source	
		Posting on mail.cypherpunks, Armadillo Remailer, "Re: Timing Attacks", 12-13-95, retrieved from internet 11-22-05, http://groups.google.com/group/mail.cypherpunks/msg/fedb10d2bcf3ff6f?dmod…	
		Posting on mail.cypherpunks, HOSELTON, Rick, "Re: Timing Cryptanalysis Attack", 12-14-95, retrieved from internet 11-22-05, http://groups.google.com/group/mail.cypherpunks/msg/470f2482c69f3212?dmo…	
		Declaration of Paul Kocher concerning the 1995 postings, KOCHER, Paul, 12-16-05	

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unqiue citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.